JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 1, 2022, p.62-74
https://publishoa.com
ISSN: 1309-3452

TTSASA: Three Tier Security against Sybil Attack

[1]Meena Bharti
Department of Computer Science and Engineering, I. K. Gujral Punjab Technical University, Kapurthala, Punjab, India. meenabharti89@gmail.com

[2]Shaveta Rani
Department of Computer Science and Engineering, Maharaja Ranjit Singh Punjab Technical University, Bathinda, Punjab, 151001, INDIA garg_shavy@mrsptu.ac.in

[3]Paramjeet Singh
Department of Computer Science and Engineering, Maharaja Ranjit Singh Punjab Technical University, Bathinda, Punjab, 151001, INDIA,param2009@mrsptu.ac.in

Received 2022 March 15; **Revised** 2022 April 20; **Accepted** 2022 May 10.

ABSTRACT

As there are limited resources in Mobile Adhoc Network (MANET) and in absence of a centralized system, security is a major concern. In a Sybil attack, intruders use multiple profiles at once or steal the identity of a trusted node in the network. This attack can cause a variety of misinterpretations in the network, such as lowering the trust of authorized nodes by utilizing their credentials, disrupting multicarrier transmission so that messages do not reach their intended destination, and so on. In the present study, a technique for the detection of Sybil attacks is proposed based on the combination of the radio range and trust value, very effectively sothat it has negligible chances of detecting false positives and false negatives. The proposed technique works on both Whitewashing attacks and simultaneous attacks. To evaluate the performance of the proposed technique, a comparison of the proposed technique is done with SQUEER, ATRP, STEAR and ETERS in terms of packet delivery ratio (PDR), throughput, average energy consumption, number of Sybil nodes detection and number of false positives. The results have shown that our proposed technique has outperformed the existing techniques.

KEYWORDS: Sybil attack, MANET, trust model, RSSI.

1. INTRODUCTION

There is mushroom growth in the use of the internet with each passing day, which requiredfora highly swift network is also increasing. MANETs are wireless networks made up of mobile nodes that communicate with one another. Each node in a MANET has a communication range[1]. It refers to a network that is devoid of infrastructure. Nodes in MANET are self-organized nodes in which all nodes play the role of the router itself. A new paradigm toward communication through highly heterogeneous networks is opportunistic networking. In an opportunistic network, nodes communicate with each other in pairs to determine the next node to reach the destination. It allows sharing of content between mobile users without the requirement of internet infrastructure. Opportunistic Networks can be challenged or delay-tolerant networks. The challenged opportunistic network contains high latency frequent disconnection, limited recourses, etc while the delay-tolerant network includes the store-carry-forwarding paradigm [2]. It is used in networks where delay in the transference of data is tolerable. The challenged opportunistic network includes VANET's, Packet Switching Networks, Wireless sensor networks and Mobile Adhoc Networks (MANET's) while delay tolerant networks include under water networks and inter-planetary networks.

Security is one of the most serious challenges with MANET due to a lack of resources and central authority. There are varieties of attacks in wireless networks. The main classification of attacks in wireless networks consists of passive attack and active attack. In the case of passive attacks, the attacker analyzes the traffic and listens to the information which is passing over the network. These attacks are difficult to detect as no modification is made to the information or network [3]. Passive attacks include eavesdropping, traffic jamming and sniffing, etc. While in the case of active attacks attacker not only hears the information flowing over the network but also can change it or intercept it [3], [4]. It includes Sybil, black hole, wormhole, vampire attack, gray hole attack, etc.

MANET network is made up of wireless nodes witha unique identity. But in the case of the Sybil node, a node can claim multiple identities [1]. It is a class of impersonatingattacks. A Sybil node can create or manage multiple identities at different locations, which can cause a problem in a network, as with multiple identities, it can control a part of the network [5]. A "Sybil attack" occurs when a hacker attempts to seize control of the entire network by breaking into other users' accounts, nodes, or machines. In the MANET, a Sybil attack means fabricating multiple false social media accounts to produce propaganda. Sybil is taken from the name of a woman whose condition was diagnosed as dissociative identity disorder[6]. For the first time, Microsoft's Brian Zill introduced the moniker 'Sybil' for this form of assault. Sybil attacks may be classified into two types: whitewashing attacks and simultaneous attacks.In case of whitewashing attack, attacker create multiple identities but one at a time. Means when attacker creates new identity it deletes previously created identity. The reason of such an attack is to clean the bad reputation of previously created identity. The trust value of previous fake identity is also got replaced with this attack. It is also called join and leave attack.In case of simultaneous attack, attackers create multiple identities and use all of them at same time. This attack is performed to disrupt the network or to use maximum resources of network like bandwidth, information etc.

A Sybil attacker can damage network in multiple ways, some of which are listed below[7]:
1. Resources of network like bandwidth, memory, computational power can be used by attacker showing multiple identities of node.
2. Routing of network will be disrupted as there are fake nodes and these fake nodes will participate in network and lead packets to non-existing paths.
3. Packets can be lost in between the network like if packet is sent towards fake node, no node will receive it and it will not reach destination.
4. Due to fake identities of node, entries in routing table will not be proper as fake nodes will also be shown in table.
5. In case of trust-based behavior scheme, the inaccuracy will increase as fake presence of fake nodes will affect the trust of other nodes also.
6. In case of voting system Sybil node can affect this system as it will have multiple identities and it can make fake polls and thus rigging the polling system.
7. It can effect on energy of network. Due to presence of fake nodes no proper path is formed for transference of packets so packets can be sent from longer path and energy of network can be diminished.
8. In case of VANET, fake identities of vehicles can be generated by attacker and false information is sent in network due to which, fake traffic jam or congestion can occur, causing diversion of traffic leads to problems to other vehicles.

There are some differences in behavior of honest nodes and Sybil nodes. Some of these behaviors differences are as follow[8]:
1. When a new node is created it will enter into radio range of other node and as soon as it will enter into radio range of other it will become its neighbor. On the other hand, Sybil node will just create new identity and it will appear abruptly in radio range of neighbor node.
2. Sybil node will try to enter at fast speed in radio range of other node so that it can penetrate more in radio range of other nodes.
3. Sybil node will try unfair means to make its trust value as high as possible.
4. In case of simultaneous attack, multiple nodes will start to appear in short span of time.
The study of these behaviors is very important as due to this we can distinguish between honest and Sybil node and can detect them.

This paper presents a Sybil attack detection technique which can handle both whitewashing as well as simultaneous attacks. This technique computes the radio range and trust value very effectively so that it has negligible chances of detecting false positives and false negatives.

The organization of the paper is as Section 1 represents the introduction to the opportunistic network and Sybil attack. Section 2 contains literature survey related to the present work. Section 3 consists of proposed work which includes assumptions of network, cluster head selection and Sybil node detection model. The theoretical evaluation of proposed work is shown in Section 4 while section 5 represents the simulation and evaluation of proposed work. Finally, Conclusion of paper is inferred in Section 6.

2. LITERATURE SURVEY

Sybil Attacks are a common occurrence in MANETs. Detecting Techniques are important for dealing with these attacks accurately.Bots or Sybil accounts, which impersonate humans, are more likely to be used to control discussions, contaminate social media with spam and disinformation, and spread fear. Social networks require Sybil detection to avoid the destruction of the network. So, various researchers have developed techniques to detect Sybil attack. Sohail Abbas et al. worked on detection lightweight Sybil attack in MANETs. In Sybil attack, attacker node can create new identity or multiple identities which can do damage in multiple ways. They detected Sybil attacker node on the basis of its entry and exit behavior. They made some observations of Sybil node on the basis that on entry it will immediately come in radio range of many nodes, it will make many neighbors immediately and it will make high trust value. They detected Sybil node on the basis of its speed of entrance. They performed two experiments of setup a threshold value of speed. Nodes which have speed less than threshold value are considered in gray zone which means legitimate nodes and nodes which have speed more than threshold value are considered as white zone means these nodes are Sybil nodes. On basis of this they differentiate normal nodes and Sybil nodes[9]. Vinicius F.S. Mota et al. explained opportunistic networks, its taxonomy and mobility models. They explained types of opportunistic networks including challenged networks and delay torrent network. Then they explained applications and projects in opportunistic network in which they cover space communication, wildlife monitoring, social applications, and cellular traffic overloading and vehicular networks. Then they explained mobility and contact patterns in which they covered most traditional model like random walk, random direction and random way point model[10]. C. Boldrini et al. [11] propose a context-based routing scheme for opportunistic networks. They present a fundamental foundation for improving and utilizing context in order to make more informed judgments. They present HiBOp, a context-based protocol, and compared this to Epidemic Routing and PROPHET, two prominent alternatives. HiBOp is likely to significantly cut resource use, according to the findings. Simultaneously, it considerably lowers the data casualty rate while maintaining transmission latency. In 2015 Khaled Rabieh et al. [12] represented cross layer scheme for detection of Sybil attack. The authors of this approach describe three stages: alarming, verification, and decision. Several strategies are utilized to suspect the presence of the Sybil node in the alarming stage. Some of alarming techniques are, in Sybil attack multiple identities of fake vehicles are create which is not always possible to be at right place sometimes mistakenly attacker can create identity of vehicle at impossible location, sometimes location or coordinates generated by attacker can overlap with other vehicles, when vehicles pass through one RSU (Road Side Unit) the information is sent to next RSU and count of number of passing vehicles at both RSUs can be matched. In verification stage verification of suspected node is done by sending packet to new location of suspected node determined by its direction and speed. The Sybil node will not be able to respond for packet in proper time and thus in decision stage decision was taken from the respond of node, time taken to respond etc that whether the node is honest node of Sybil node. Another unique lightweight solution for mitigating Sybil attacks in VANETs is presented. The proposed technique employs secret key cryptography and authenticity between Roadside Units (RSUs) as well as on-road cars to ensure that no hostile automobile can acquire multiple identities within the network. This method does not require administrators for RSUs or Certification Authorities (CAs), so it employs the fewest message possible to communicate with RSUs, enabling the method efficient and productive [13]. Furthermore, for Sybil attack detection in MANET, the architecture of a fuzzy based cooperative verification procedure is given. If the originating stations wish to connect with a target that uses this strategy, they must rely on the surveillance nodes to communicate information like range, direction, and RSS variation with the two separate neighbor nodes in a cooperative manner. It uses fuzzy logic to recognize the weakly or severely suspicious node based on the analysis of the data gathered. But since Sybil assault has been proven by a cooperative swap of activities and operations, there is a prospect of reducing false and missed identification. The cost from overhearing the entire node is decreased utilizing the developed model, according to the findings[14]. A Bloom filter and Puf based technique is to detect the Sybil attack. Bloom filter is formed through hashing authorized user's identity and each node contains bloom filter table that assists to detect Sybil nodes[15]. A detailed classification of Sybil attack detection techniques has been presented in [7]. There are various methods to detect Sybil attack. Each method has its own merits as summarized in Table1.

3. PROPOSED WORK

The growth of the internet is at a very fast pace due to which sensor nodes are used to carry sensitive data sometimes. The security of such data is a major concern. Sybil attack is a risky attack in which an attack node joins the network several times while posing as someone else. The Sybil attack is capable of disrupting networks, can also affect the online voting system. The Sybil attack can be white-washing and simultaneous. In a recent study, we have tried to detect both types of Sybil attacks by combining RSSI and trust-based Sybil attack detection. We are proposing 3 tier security for this purpose. In the first tier, RSSI-based security is provided, in the second layer local level trust is computed while in the third-tier cluster level and inter-cluster level trust is computed.

Table1: Sybil Attack Detection Techniques

Sybil Attack Detection Types	Count Measures Developed	Basic Technique
Artificial Intelligence	[16]–[18]	Detecting the Sybil node by learning, cooperation, sharing knowledge etc.
Encryption	[13], [19], [20]	Key management and creation for secure Identity management
Received Signal Strength Indicator (RSSI)	[21], [22], [23, p.], [23]	Calculates the distance between two identities' locations and determines the relationship between the unique identities of surrounding nodes.
Trust value	[5], [24], [25, p.], [26]	Predicting the node's behavior by computing trust values by making cluster network
MultiKernel	[27], [28]	Examine Radio source to construct channel vector from the source node and further gap is computed.
Rule-based Anomaly	[29], [30]	Rules are formed based on the past experience and behavior.
Bloom filter and PUF based	[15], [31]	Bloom filter is formed through hashing authorized user's identity and each node contains bloom filter table that assists to detect Sybil nodes

3.1. ASSUMPTIONS OF NETWORK

Figure 1 depicts the network that was employed in this study. There is one basestation that can place or remove nodes from the network. It also initializes the initial energy of the network. The Base station acts as sink also as cluster heads collects message from sensor nodes in their cluster and send to base station.

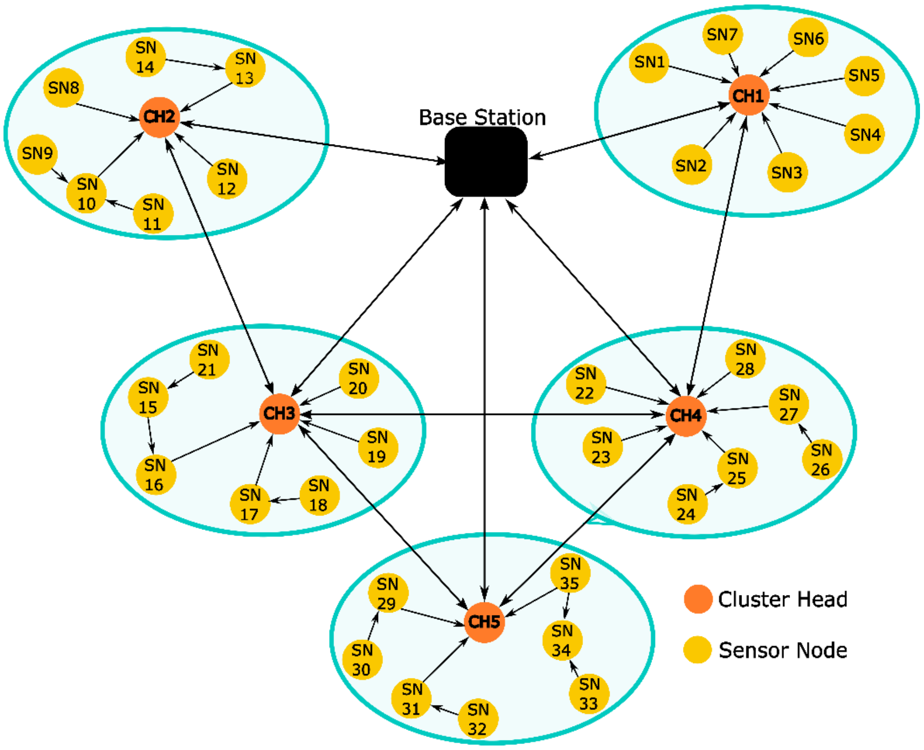

Figure 1: Clustered Network

The nodes can send message to cluster head directly or through other nodes. To maintain energy of network it is assumed that the nodes having more than 20% of initial energy will take part in routing while nodes with energy less than 20% of initial energy will perform basic activities only. The consumption of energy of cluster head is more as compared to sensor nodes so cluster heads will be changed after a certain period of time to do load balancing. Two arrays will be maintained by each node one is for trust values of all nodes of the network and the other is of Sybil or malicious nodes. The trust value lies in the range of$[0, \varpi - 1]$and the initial trust value assigned by BS is$[(\varpi - 1)/2]$. If the trust value $(\mathcal{T})$ of sensor nodes is greater or equal to $(\varpi - 1)/2$ SN is considered as an honest node. For purpose of routing proactive routing, techniques are used within a cluster as in the case of proactive routing, routing tables are maintained, so routing is fast and less energy is consumed. While communication in inter-cluster is done using a reactive approach. When nodes transmit packets, their energy is consumed which is known as transmission energy. Let's assume a node has to send k bits/packet to another node which is ∂ meters away then Eq. (1) can be used to calculate transmission energy as [32]

$$E_{T,X}(k,d) = \left\langle \begin{matrix} k \times E_{elec} + k \times \in_{fs} \times \partial^2 \\ k \times E_{elec} + k \times \in_{amp} \times \partial^4 \end{matrix} \middle| \begin{matrix} \partial \leq \partial_0 \\ \partial > \partial_0 \end{matrix} \right\rangle \quad (1)$$

Where, E_{elec} is the energy used per bit in transmission or receiving of packets, $\in_{amp}$, and $\in_{fs}$ are multipath fading model and free space model respectively. Similarly, the energy consumed in receiving a k bits/packet can be defined in Eq. (2)

$$E_{RX}(k) = k \times E_{elec} \qquad (2)$$

3.2. CLUSTER HEAD SELECTION

When the working of network starts initially cluster heads are selected. Various researches have worked on choosing cluster heads efficiently. The cluster head selection is based on distance with neighbor nodes, residual energy, the highest degree of a number of neighbors etc. In the present work, we have tried to choose cluster head efficiently on the basis of link quality, residual energy and number of neighbors and mobility of node. In the case of MANET, sensor nodes are moving so the cluster head should be will less mobility or static so that it can serve the cluster well. Moreover, the cluster head has more load than other nodes so energy consumption is high. So residual energy is also taken factor while choosing cluster head. The cluster head is changed after periodic interval of time to do load balancing. Algorithm 1 contains the cluster head selection algorithm.

Algorithm 1: Cluster Head Selection

```
Input: Sensor nodes, their co-ordinates and energy
Output: Cluster heads

1. For each $i \in N$, find the number of neighbors of each sensor node and store in array D.
       $D = \{d_1, d_{2,} d_3 \dots\dots\dots\dots\dots\dots\dots\dots\ d_N$
2. Find the mobility of nodes and store in array M.
       $M = \{m_1, m_{2,} m_3 \dots\dots\dots\dots\dots\dots\dots\dots\ m_N$
3. Find the residual energy of nodes and store in array E.
       $E = \{e_1, e_{2,} e_3 \dots\dots\dots\dots\dots\dots\dots\dots\ e_N$
4. Calculate link quality Q.
       $Q_i = \frac{number\ of\ packet\ send\ by\ SN_i}{number\ of\ packets\ recieved\ by\ BS}$
5. Calculate cluster value CV
       $CV_i = w_1 \times d_i + w_2 \times \frac{1}{m_i} + w_3 \times e_i + w_4 \times Q_i$
   Where $w_1 + w_2 + w_3 + w_4 = 1$
6. Cluster head CH = max $\{CV_1, CV_2, CV_3, \dots\dots\dots\dots\dots\dots CV_N\}$
7. End loop
8. Repeat steps 1 to 7 to select new Cluster head after certain period of time.
```

3.3. DETECTION MODEL

Three-tier security is proposed in the present work. The first tier consists of RRSI based detection. In this case, it is considered that when a legitimate node say SN(M) enters in the radio range of another node say SN(N) it will slowly enter in its radio range and while Sybil node says SN(O) will appear abruptly anywhere in the network. So, when node SN(N) will firstly observe node SN(M) it will be penetrated shallow in radio range of SN(N) while when Sybil node SN(O) will be firstly observed by SN(N) it will be penetrated deeply in radio range of SN(N). This tier is capable of detecting Sybil node at an early stage but there is a chance of false positive in this case. Sometimes while entering the radio range of node SN (N) it can be a chance that the node has lost a connection that why is observed at a penetration value higher than a threshold value. To overcome this problem the threshold value is kept higher due to which some of the Sybil nodes can remain undetected. Such types of nodes will be detected in the second tier. In the second tier, the local level trust value is calculated by neighboring nodes after a periodic interval of time. Local trust is based upon successful packets transferred by a node. Cluster level trust is based on trust of all nodes in cluster and also inter cluster trust is calculated for this purpose. The algorithm for calculation of trust and detection of Sybil nodes is provided in Algorithm 2.

Algorithm 2: Detection of Sybil Nodes

```
Input: Sensor nodes, theircoordinates, initial energy and trust value
Output: Detection of Sybil nodes.

1. Initialize co-ordinates, initial energy and trust value of sensor nodes.
2. Communication of nodes start
3. Using Algorithm 1 find cluster heads
4. Find neighbors for SNs
5. Communication and forwarding of packets in SNs start
6. If $node_{energy} > 20\ \%\ of\ initial\ energy\ (\mathbb{E})$
```

```
        Sensor node will part in routing
        Else
        Sensor node will perform basic operations only
    7.  Check energy after periodic interval of time.
    8.  Calculate RSS of SN value at entry
    9.  If RSS > $\text{Threshold}_{\text{RSS}}$
        Put this node in malicious list and broadcast message
        Base station will remove this node
    10. Compute local trust for time slot $(\Delta t)$, say node SN(M) is calculating local trust for it neighbor SN(N)
        $$\mathcal{L}_{M,N}(\Delta t) = \left[\varpi \times \left(\frac{C_{M,N}(\Delta t) + 1}{C_{M,N}(\Delta t) + I_{M,N}(\Delta t) + 2}\right)^{\left(\frac{I_{M,N}(\Delta t)+1}{C_{M,N}(\Delta t)+ I_{M,N}(\Delta t)+2}\right)}\right]$$
        Where $C_{M,N}(\Delta t)$ is number of correct packets forwarded by SN(N) which were send by SN(M), and
        $I_{A,B}(\Delta t)$is number of packets not forwarded by B which were send by SN(M)
    11. While $\mathcal{L}_{M,N}(\Delta t) \geq \left[\frac{\varpi - 1}{2}\right]$
        Transmission of packet will go on normally
    12. If $\mathcal{L}_{M,N}(\Delta t) < \left[\frac{\varpi - 1}{2}\right]$
        Node A will send message to cluster head.
    13. Cluster head will calculate cluster level trust
        $$\mathbb{C}_{CH,N}(\Delta t) = \sum_{i=1}^{\eta} \frac{\mathcal{L}_{i,N}(\Delta t)}{\eta}$$
        Where $\eta$ is number of nodes of cluster.
    14. Then cluster head will find inter-cluster trust by asking from other cluster heads.
        $$\text{IT}_{CH,N}(\Delta t) = \sum_{i=1}^{\eta_C} \frac{\mathbb{C}_{i,N}(\Delta t)}{\eta_C}$$
        Where $\eta_C$ is number of clusters in network.
    15. Final trust value for node N will be
        $$\Im_N(\Delta t) = \alpha \times \mathbb{C}_{CH,N}(\Delta t) + \beta \times \text{IT}_{CH,N}(\Delta t)$$
    16. If $\Im_N(\Delta t) \geq \left[\frac{\varpi - 1}{2}\right]$
        Normal communication will take place.
        Else
        CH will inform all nodes about node SN(N)
        All nodes will add node SN (N) in malicious array list.
```

4. THEORETICAL EVALUATION OF LOCAL TRUST

In this section we have done the theoretical analysis of local trust. It will proof resistance to malicious attack of proposed model.

Theorem - The local trust is robust against Sybil attack.

Proof– There are two possibilities in which Sybil node can trick network.

1. **Hypothesis 1**: When $I_{M,N}(\Delta t) > C_{M,N}(\Delta t)$ and $\mathcal{L}_{M,N}(\Delta t) \geq \left[\frac{\varpi - 1}{2}\right]$

   $I_{M,N}(\Delta t) > C_{M,N}(\Delta t) => I_{M,N}(\Delta t) = C_{M,N}(\Delta t) + \gamma$

Substitute these values in local trust formula

$$\mathcal{L}_{M,N}(\Delta t) = \left[\varpi \times \left(\frac{C_{M,N}(\Delta t)+1}{C_{M,N}(\Delta t)+ (C_{M,N}(\Delta t)+\gamma)+2}\right)^{\left(\frac{(C_{M,N}(\Delta t)+\gamma)+1}{C_{M,N}(\Delta t)+(C_{M,N}(\Delta t)+\gamma)+2}\right)}\right]$$

$$=> L_{M,N}(\Delta t) = \left[\varpi \times \left(\frac{C_{M,N}(\Delta t)+1}{2 \times C_{M,N}(\Delta t)+\gamma+2}\right)^{\left(\frac{C_{M,N}(\Delta t)+\gamma+1}{2 \times C_{M,N}(\Delta t)+\gamma+2}\right)}\right]$$

For simplification let'sconsider $v = 4$, $\gamma = 8$, Then

$$\mathcal{L}_{M,N}(\Delta t) = \left[4 \times \left(\frac{C_{M,N}(\Delta t)+1}{2 \times C_{M,N}(\Delta t)+ 8+2}\right)^{\left(\frac{C_{M,N}(\Delta t)+8+1}{2 \times C_{M,N}(\Delta t)+8+2}\right)}\right]$$

$$=> L_{M,N}(\Delta t) = \left[4 \times \left(\frac{C_{M,N}(\Delta t)+1}{2 \times C_{M,N}(\Delta t)+ 10}\right)^{\left(\frac{C_{M,N}(\Delta t)+9}{2 \times C_{M,N}(\Delta t)+10}\right)}\right]$$

Suppose $C_{M,N}(\Delta t)$ =2 then $\mathcal{L}_{M,N}(\Delta t)$ = 1.192 which is lower than $\left[\frac{\varpi-1}{2}\right]$ = 1.5, this is contradiction to the Hypothesis1. Similarly, for all values of $C_{M,N}(\Delta t), \mathcal{L}_{M,N}(\Delta t) < \left[\frac{\varpi-1}{2}\right]$ which implies that for all values of $I_{M,N}(\Delta t) > C_{M,N}(\Delta t)$ the local trust $\mathcal{L}_{M,N}(\Delta t) < \left[\frac{\varpi-1}{2}\right]$

Hypothesis 2: When $I_{M,N}(\Delta t) < C_{M,N}(\Delta t)$ and $\mathcal{L}_{M,N}(\Delta t) < \left[\frac{\varpi-1}{2}\right]$

$I_{M,N}(\Delta t) < C_{M,N}(\Delta t) \; => I_{M,N}(\Delta t) = C_{M,N}(\Delta t) - \gamma$

For simplification $v = 4$, Putting these values in local trust formula.

$$\mathcal{L}_{M,N}(\Delta t) = \left[4 \times \left(\frac{C_{M,N}(\Delta t)+1}{C_{M,N}(\Delta t)+ (C_{M,N}(\Delta t)-\gamma)+2}\right)^{\left(\frac{(C_{M,N}(\Delta t)-\gamma)+1}{C_{M,N}(\Delta t)+(C_{M,N}(\Delta t)-\gamma)+2}\right)}\right]$$

$$=> L_{M,N}(\Delta t) = \left[4 \times \left(\frac{C_{M,N}(\Delta t)+1}{2 \times C_{M,N}(\Delta t)-\gamma+2}\right)^{\left(\frac{C_{M,N}(\Delta t)-\gamma+1}{2 \times C_{M,N}(\Delta t)-\gamma+2}\right)}\right]$$

Consider $\gamma = 8$, then

$$\mathcal{L}_{M,N}(\Delta t) = \left[4 \times \left(\frac{C_{M,N}(\Delta t)+1}{2 \times C_{M,N}(\Delta t)-6}\right)^{\left(\frac{C_{M,N}(\Delta t)-7}{2 \times C_{M,N}(\Delta t)-6}\right)}\right]$$

Suppose $C_{M,N}(\Delta t) = 10$ then $\mathcal{L}_{M,N}(\Delta t) = 3.79$ which is higher than $\left[\frac{\varpi-1}{2}\right]$ = 1.5, this is contradiction to the Hypothesis2. Similarly, for other values also if$I_{M,N}(\Delta t) < C_{M,N}(\Delta t), \mathcal{L}_{M,N}(\Delta t) \geq \left[\frac{\varpi-1}{2}\right]$.

As both hypotheses are capable of catching Sybil nodes hence it can be proved that proposed scheme is robust to Sybil attack.

5. SIMULATION AND EVALUATION

The simulation of proposed work is carried out on MATLAB R2018a. The proposed scheme is compared with SQUEER[33], ATRP[34], STEAR[35], ETERS in terms of PDR, Throughput, Average energy consumed, Detection accuracy of Sybil nodes, number of false positives. The performance of network is checked by increasing number of Sybil nodes. The experiment is carried out on network by varying number of nodes from 100 to 400. Table 2 lists the parameters that were utilized in the simulation.

Table 2: List of simulation parameters

List of Parameters	Values
Network area	1000m x 1000m
Simulation Time	1000s
Number of sensor nodes	100-500
Radio range of sensor nodes	20m
Initial Energy	5J
Range of trust(r)	4
Size of Packet	512 bytes
Number of Sybil nodes	10% - 60%

5.1. Packet Delivery Ratio (PDR) – It means ratio of number of packets reached at destination to total number of packets forwarded. The packets RREP and RREQ are also included in formula to find PDR. It is desirable that maximum number of packets reach at destination. High PDR means more reliable is the network. The comparative analysis of proposed work with existing techniques is shown in Figure 2.

5.2. Average Energy Consumed- When a node transmits or receives a packet some of energy is consumed. When there are large number Sybil nodes more energy is consumed as sender has to retransmit packet if it doesn't get acknowledgement after certain period of time. So early detection of Sybil nodes causes less consumption of energy. Apart from this selection of shortest path also consumes less energy as a smaller number of nodes will transmit packet on the route. The comparative analysis of proposed scheme with existing techniques in terms of Average Energy Consumed is shown in Figure 3.

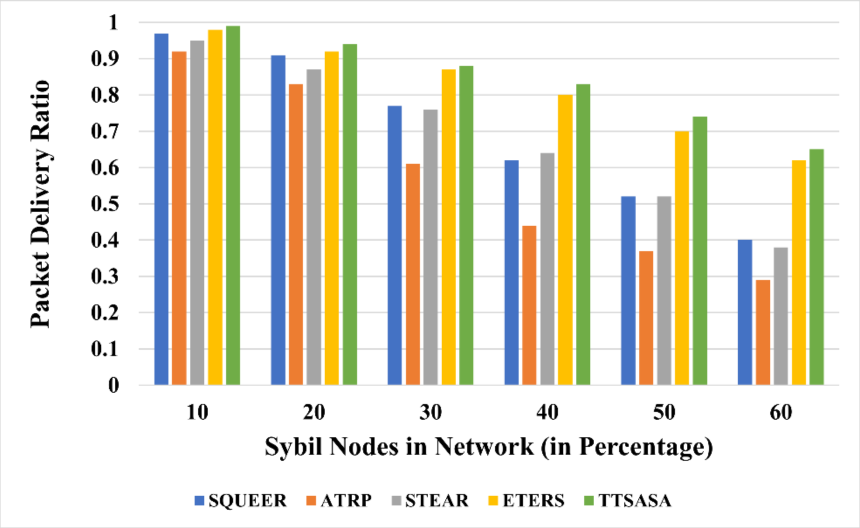

Figure 2: Packet Delivery Ratio with varying percentage of Sybil Nodes.

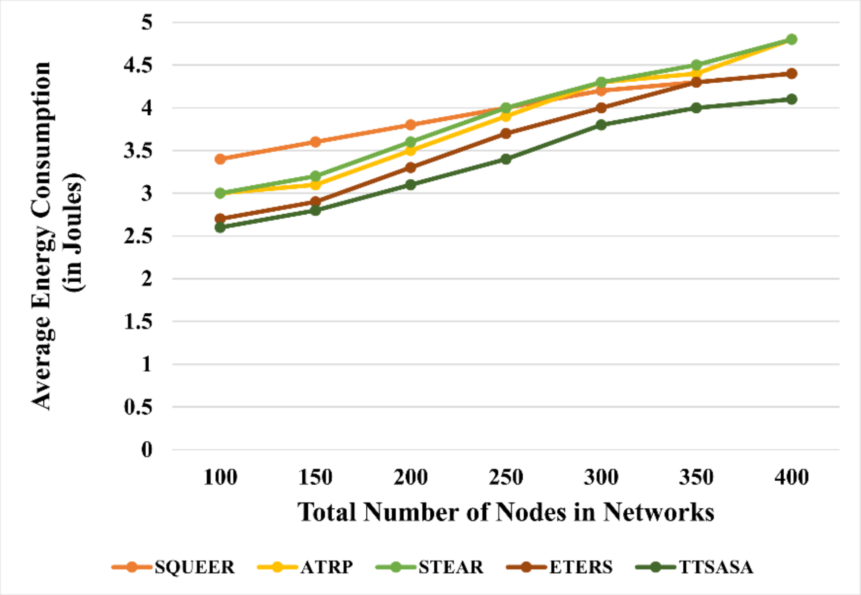

Figure 3: Average Energy Consumed with varying number of nodes of network under attack conditions

5.3. Network Throughput – It is the ratio of number of packets delivered to destination per unit time. It is desirable to have high throughput. The comparative analysis of network throughput of proposed scheme with existing techniques is shown in Figure 4. Some might confuse with Network Throughput and PDR. To clarify the difference between two let's consider two cases. In case 1, let's consider packets are at initial stage but due to buffer or wait time packets are not sent further. This will not affect PDR as packets hasn't entered in the system yet but it will affect throughput of network as number of packets reached at destination per unit time will decrease. In another case, let's consider packet delivery is failed 2 or 3 times, it will not affect much on throughput but will affect PDR as packets have entered in network but not reached at destination.

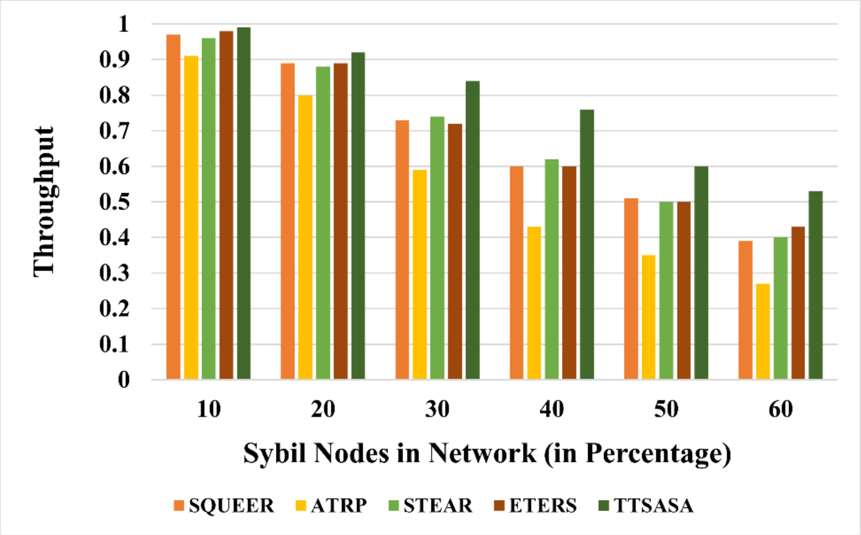

Figure 4: Network Throughput with varying number of malicious nodes

5.4. Detection Accuracy of Sybil nodes- It means how many Sybil nodes are detected accurately in a network. To calculate detection accuracy number sybil nodes are induced with varying percentage to see its effect on detection accuracy. The comparative analysis of detection accuracy of proposed work with existing techniques is shown in Figure 5.

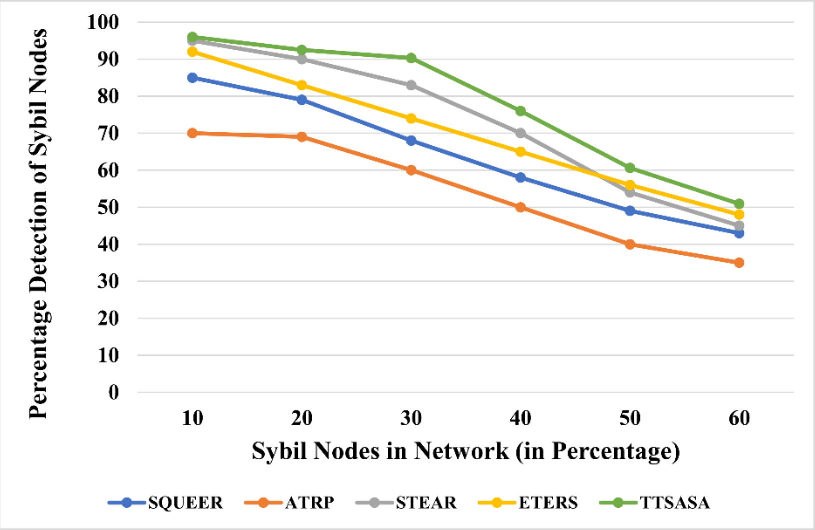

Figure 5: Detection Accuracy with varying number of Sybil Nodes

5.5. Number of False Positives- It means how many nodes are wrongly detected as Sybil node. It is desirable to have low false positive. Low number of false positive means more reliable is the algorithm. The comparative analysis of number of false positives with existing techniques is shown in Figure 6.

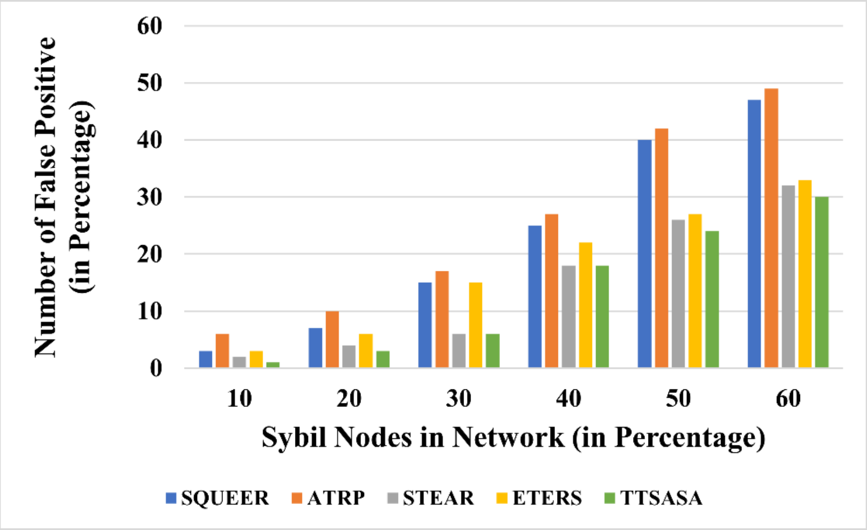

Figure 6: Number of False Positives with varying number of SybilNodes.

As depicted from Figure 2 to Figure 6 the packet delivery ratio, network throughput and detection accuracy of Sybil nodes is higher as compared to existing techniques while energy consumed and false positives are lower than existing techniques. However, the number of false positives of proposed work is similar to ETERS as they also have used dynamic scheme. But proposed work is consuming low energy as compared to ETERS. It is because we have used combination of RSSI and trust-based Sybil node detection. RSSI value identifies Sybil nodes early, therefore certain nodes are discovered early, which decreases energy usage, which needs to be due to source node not delivering packets and retransmitting packets.

6. CONCLUSION AND FUTURE SCOPE

As there is fast-growing internet world, sometimes, transmission of data is done through the sensor nodes. Security of data is a crucial task as sometimes nodes carries critical information. Sybil nodes contains fake identities and try to disrupt working of network by affecting voting, data aggression etc. In such situation providing security to network becomes more complicated. In this study, we have proposed a technique based on combination of RSSI value and trust-based Sybil attack detection so that we can take advantages of both techniques while minimizing their disadvantages. We have provided 3 tier security of network. In first tier RSSI based Sybil node detection is used. In second tier direct trust is calculated while in third tier indirect trust is calculated. We have compared our proposed technique with SQUEER, ATRP, STEAR and ETERS in terms of packet delivery ratio, average energy consumed, throughput, number of Sybil nodes detection and number of false positives. The results have shown that our proposed technique is efficient than pre-existing techniques. In future, we want to enhance our work on IOT based applications.

ACKNOWLEDGMENT

The authors wish to thank many anonymous referees for their suggestions to improve the paper. Meena Bharti would like to thank I.K. Gujral Punjab Technical University for offering the Ph.D. course in Computer Science & Engineering and providing support to access the resources for research.

REFERENCES

[1] A. S. Sastry, S. S. Chitlapalli, and S. Akhila, “Work-in-Progress: A Novel Approach to Detection and Avoid Sybil Attack in MANET,” in *International Conference on Remote Engineering and Virtual Instrumentation*, 2019, pp. 429–441.

[2] Y. Mao, C. Zhou, Y. Ling, and J. Lloret, “An optimized probabilistic delay tolerant network (DTN) routing protocol based on scheduling mechanism for internet of things (IoT),” *Sensors*, vol. 19, no. 2, p. 243, 2019.

[3] U. Ahamed and S. Fernando, “Identifying the impacts of active and passive attacks on network layer in a mobile ad-hoc network: a simulation perspective,” *Int. J. Adv. Comput. Sci. Appl. IJACSA*, vol. 11, no. 11, 2020.

[4] S. Sankara Narayanan and G. Murugaboopathi, “Modified secure AODV protocol to prevent wormhole attack in MANET,” *Concurr. Comput. Pract. Exp.*, vol. 32, no. 4, p. e5017, 2020.

[5] P. Otte, M. de Vos, and J. Pouwelse, “TrustChain: A Sybil-resistant scalable blockchain,” *Future Gener. Comput. Syst.*, vol. 107, pp. 770–780, 2020.

[6] P. Roy and M. Sood, “Implementation of Ensemble-Based Prediction Model for Detecting Sybil Accounts in an OSN,” in *International Conference on Innovative Computing and Communications*, 2021, pp. 709–723.

[7] A. S. Koleshwar, S. S. Sherekar, V. M. Thakare, and A. Kanhe, “Analytical Classification of Sybil Attack Detection Techniques,” in *Intelligent Data Communication Technologies and Internet of Things*, Springer, 2021, pp. 89–98.

[8] A. Alharbi, M. Zohdy, D. Debnath, R. Olawoyin, and G. Corser, “Sybil attacks and defenses in internet of things and mobile social networks,” *Int. J. Comput. Sci. Issues IJCSI*, vol. 15, no. 6, pp. 36–41, 2018.

[9] S. Abbas, M. Merabti, D. Llewellyn-Jones, and K. Kifayat, “Lightweight sybil attack detection in manets,” *IEEE Syst. J.*, vol. 7, no. 2, pp. 236–248, 2012.

[10] V. F. Mota, F. D. Cunha, D. F. Macedo, J. M. Nogueira, and A. A. Loureiro, “Protocols, mobility models and tools in opportunistic networks: A survey,” *Comput. Commun.*, vol. 48, pp. 5–19, 2014.

[11] C. Boldrini, M. Conti, J. Jacopini, and A. Passarella, “Hibop: a history based routing protocol for opportunistic networks,” in *2007 IEEE international Symposium on a world of wireless, mobile and multimedia networks*, 2007, pp. 1–12.

[12] K. Rabieh, M. M. Mahmoud, T. N. Guo, and M. Younis, “Cross-layer scheme for detecting large-scale colluding Sybil attack in VANETs,” in *2015 IEEE International Conference on Communications (ICC)*, 2015, pp. 7298–7303.

[13] M. Khalil and M. A. Azer, “Sybil attack prevention through identity symmetric scheme in vehicular ad-hoc networks,” in *2018 Wireless Days (WD)*, 2018, pp. 184–186.

[14] H. Rajadurai and U. D. Gandhi, “Fuzzy based collaborative verification system for Sybil attack detection in MANET,” *Wirel. Pers. Commun.*, vol. 110, no. 4, pp. 2179–2193, 2020.

[15] C. Pu and K.-K. R. Choo, “Lightweight Sybil Attack Detection in IoT based on Bloom Filter and Physical Unclonable Function,” *Comput. Secur.*, vol. 113, p. 102541, 2022.

[16] A. Mehbodniya, J. L. Webber, M. Shabaz, H. Mohafez, and K. Yadav, “Machine Learning Technique to Detect Sybil Attack on IoT Based Sensor Network,” *IETE J. Res.*, pp. 1–9, 2021.

[17] M. Mounica, R. Vijayasaraswathi, and R. Vasavi, “Detecting sybil attack in wireless sensor networks using machine learning algorithms,” in *IOP Conference Series: Materials Science and Engineering*, 2021, vol. 1042, no. 1, p. 012029.

[18] C. H. Quevedo, A. M. Quevedo, G. A. Campos, R. L. Gomes, J. Celestino, and A. Serhrouchni, “An intelligent mechanism for sybil attacks detection in vanets,” in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1–6.

[19] A. S. S. Thuluva, M. S. Somanathan, R. Somula, S. Sennan, and D. Burgos, “Secure and efficient transmission of data based on Caesar Cipher Algorithm for Sybil attack in IoT,” *EURASIP J. Adv. Signal Process.*, vol. 2021, no. 1, pp. 1–23, 2021.

[20] S. S. Vinayagam and V. Parthasarathy, “A secure restricted identity-based proxy re-encryption based routing scheme for sybil attack detection in peer-to-peer networks,” *J. Comput. Theor. Nanosci.*, vol. 15, no. 1, pp. 210–221, 2018.

[21] A. Angappan, T. P. Saravanabava, P. Sakthivel, and K. S. Vishvaksenan, “Novel Sybil attack detection using RSSI and neighbour information to ensure secure communication in WSN,” *J. Ambient Intell. Humaniz. Comput.*, vol. 12, no. 6, pp. 6567–6578, 2021.

[22] M. Sadeghizadeh, “A lightweight intrusion detection system based on RSSI for sybil attack detection in wireless sensor networks,” *Int. J. Nonlinear Anal. Appl.*, vol. 13, no. 1, pp. 305–320, 2022.

[23] Y. Yao *et al.*, “Multi-channel based Sybil attack detection in vehicular ad hoc networks using RSSI,” *IEEE Trans. Mob. Comput.*, vol. 18, no. 2, pp. 362–375, 2018.

[24] A. Anwar, T. Halabi, and M. Zulkernine, “Cloud-based Sybil Attack Detection Scheme for Connected Vehicles,” in *2019 3rd Cyber Security in Networking Conference (CSNet)*, 2019, pp. 114–121.

[25] A. Rhamdhan and F. Hidayat, “Hybrid Trust-based Defense Mechanisms Against Sybil Attack in Vehicular Ad-hoc Networks,” 2020.

[26] A. Tandon and P. Srivastava, “Trust-based enhanced secure routing against rank and sybil attacks in IoT,” in *2019 Twelfth International Conference on Contemporary Computing (IC3)*, 2019, pp. 1–7.

[27] Q. Li and M. Cheffena, “Exploiting dispersive power gain and delay spread for sybil detection in industrial wsns: a multi-kernel approach,” *IEEE Trans. Wirel. Commun.*, vol. 18, no. 3, pp. 1805–1818, 2019.

[28] K. Nitya, B. Nancharaiah, and S. Venkatesan, “A Comparative Survey on Secure Energy Efficient Routing in WSNs,” in *2021 5th International Conference on Information Systems and Computer Networks (ISCON)*, 2021, pp. 1–5.

[29] M. C. Belavagi and B. Muniyal, “Improved Intrusion Detection System using Quantal Response Equilibrium-based Game Model and Rule-based Classification,” *Int. J. Commun. Netw. Inf. Secur.*, vol. 13, no. 1, pp. 1–8, 2021.

[30] K. P. Singh and N. Kesswani, “An Anomaly-Based Intrusion Detection System for IoT Networks Using Trust Factor,” *SN Comput. Sci.*, vol. 3, no. 2, pp. 1–9, 2022.

[31] B. Mbarek, N. Sahli, and N. Jabeur, “BFAN: A Bloom Filter-Based Authentication in Wireless Sensor Networks,” in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, 2018, pp. 304–309.

[32] T. M. Behera, U. C. Samal, and S. K. Mohapatra, “Energy-efficient modified LEACH protocol for IoT application,” *IET Wirel. Sens. Syst.*, vol. 8, no. 5, pp. 223–228, 2018.

[33] T. Kalidoss, L. Rajasekaran, K. Kanagasabai, G. Sannasi, and A. Kannan, “QoS aware trust based routing algorithm for wireless sensor networks,” *Wirel. Pers. Commun.*, vol. 110, no. 4, pp. 1637–1658, 2020.

[34] N. A. Khalid, Q. Bai, and A. Al-Anbuky, “Adaptive trust-based routing protocol for large scale WSNs,” *IEEE Access*, vol. 7, pp. 143539–143549, 2019.

[35] B. M. Thippeswamy, S. Reshma, V. Tejaswi, K. Shaila, K. R. Venugopal, and L. M. Patnaik, “STEAR: Secure trust-aware energy-efficient adaptive routing in wireless sensor networks,” *J. Adv. Comput. Netw.*, vol. 3, no. 2, 2015.